LA-UR-99-3809

*Approved for public release;
distribution is unlimited.*

Title:

Tamper detection requires dedication

Author(s):

Roger G. Johnston

Submitted to:

http://lib-www.lanl.gov/la-pubs/00460170.pdf

Tamper detection requires dedication

Roger G. Johnston, Ph.D., CPP

Vulnerability Assessment Team
Los Alamos National Laboratory
MS J565, Los Alamos, NM 87545 USA
phone: 505-667-7414
fax: 505-665-4631
email: rogerj@lanl.gov

In the Camelot legend, King Arthur relied on his magic sword (Excalibur) and Merlin the Magician to help protect himself and his kingdom. In the end, however, all his belief in magic failed to prevent disaster. There's a lesson there.

Revenue protection and loss prevention are hot topics nowadays in the utility industry. Tamper-indicating seals are often used to help detect theft and diversion, as well as meter tampering. Unlike locks, seals are not meant to physically impede unauthorized access or entry. Instead, they are meant to record that it took place.

The good news about seals is that--if used correctly--they can be very effective at detecting tampering. The bad news is that using them correctly can take a lot of work. You can't mindlessly slap seals on a meter and expect them to magically solve all your theft and tampering problems.

Let's review the bad news about seals. Then I'd like to offer some suggestions for how to use them effectively.

Bad News

The first piece of bad news is that you can't use seals effectively in a vacuum. You must undertake a fair amount of introspection. Many seal users--in and outside the utility industry--are remarkably vague on exactly what their tamper detection program is all about. It is not possible to optimize your chances for tamper detection without a thorough understanding of the specific goals of your security program, your likely adversaries (know thine enemy!), the personnel and resources you are willing to devote to the task, the consequences of a security failure, and what you will do when you find evidence of tampering. These issues need to be reviewed on a regular basis.

More Bad News

Choosing an appropriate seal is complicated. In my experience, most seal users (commercial or government) choose seals based on the following criteria, in order of decreasing priority:

1. unit cost
2. familiarity/tradition
3. environmental durability
4. ease of use
5. gossip--a colleague (or the sales guy) says something nice about the seal, or something bad about a competing seal.

Attributes such as vulnerability to attack, and tamper-detection reliability often don't even make the list! This is probably because they are much harder to evaluate.

In extreme (but all too common) cases, seal users become so obsessed with the unit cost of a seal, that they ignore everything else. This is unfortunate because it encourages seal manufacturers and developers to concentrate on making cheap seals at the cost of good security. It is also ill-advised because the unit cost of a seal is often one of the least important economic factors. Costs associated with effective seal procurement, installation, inspection, record keeping, disposal, and training can be far larger. Not to mention the costs of undetected theft!

Vulnerabilities

Unhappily, seal choice is further complicated by the fact that there simply is no such thing as a "tamper-proof" or "impossible to defeat" seal. Never mind what some some seal manufacturers and vendors might tell you.

To "defeat" a seal means to open it, gain access to what it is protecting, and then reseal it (or else replace it with a counterfeit)--all without being detected. To "attack" a seal means to try to defeat it.

The Vulnerability Assessment Team (VAT) at Los Alamos National Laboratory has studied 120 different seals in detail. Most are in widespread use. They include both expensive and inexpensive products, and commercial as well as government-developed seals. The VAT has shown how all 120 seals can be quickly and easily defeated using low-tech methods, tools, and supplies available to almost anyone. Ironically, high-tech seals are sometimes easier to defeat than simple low-tech mechanical seals!

The findings of easy-to-exploit seal vulnerabilities are not unique to the VAT. Others have made similar observations over the years. The work of the VAT differs only in its breadth.

More Bad News Regarding Personnel

And yet more bad news! Your tamper-detection program is no better than the people you put out in the field. If you pay minimum wages to a demoralized, poorly trained, unmotivated crew of seal installers and inspectors who take no personal interest in your loss problems, you will not be effective at detecting tampering.

Why Bother?

So if seals are full of bad news, why bother? The answer is that seals (unlike locks) can actually detect tampering quite well, but only if you are willing to do some hard work. You only get out of seals what you put in.

Using Seals Effectively

To use seals effectively: You must think carefully about why you are using seals. You need to pick them intelligently. You have to keep very accurate records and follow careful procedures. You should understand the vulnerabilities associated with the specific seals you are using and look for the most likely attacks. (If you do that, most seal vulnerabilities either go away, or are greatly reduced.) You must effectively train and motivate your personnel.

Most painful of all, you have to pay attention and you have to think. Despite the fantasies of some seal users and manufacturers, no seal will do that for you.

General Suggestions

The best advice for optimizing a tamper detection program depends critically on details of the application, the seal user and his goals, and the seal being used. There are, however, some general suggestions that seem to have a fairly broad range of applicability. They apply whether your seal installers and inspectors are employees, or contract personnel.

Not all of these suggestions are automatically missing from any given seal program. Most seal users, however, would probably benefit from at least a renewed emphasis on some of these matters.

(1) Tell seal manufacturers and vendors that you are interested in seal security, not just cost. (And mean it!) Encourage them to develop new seals designed specifically for your application. Better seals are possible!

(2) Many seal manufacturers claim to protect seal logos and serial numbers from unauthorized purchasers. Test this yourself covertly. It’s not always true.

(3) Only a small number of personnel within the utility should be authorized to order, store, checkout, and dispose of security seals.

(4) Show your seal installers and inspectors examples of attacked seals. Inspectors should be familiar with the most likely attack scenarios associated with the specific seal they are using, and look or test for them. Vague instructions to, for example, "look for signs of tampering" are not satisfactory.

(5) Encourage your personnel to think about how to attack your seals and tamper detection program. Whether the attacks they devise are practical is less important than getting them to think like an adversary.

(6) To the extent possible, seek to engage your seal installers and inspectors intellectually and emotionally in the task of “catching the bad guys”. Explain to them the importance of revenue protection and loss prevention. Explain the reasons for the various seal procedures. Hold contests and demonstrations of prowess.

(7) Treat your seal installers and inspectors well. Having disgruntled security personnel is a classic way that security programs fail.

(8) Give them a reason to pay attention. Generously and immediately reward seal installers and inspectors who find legitimate problems. Employees who save the utility from theft and loss of revenue are heroes and should be hailed as such in the company newsletter, or even the local newspaper.

(9) Test your seal installers and inspectors (and your tamper detection program) on a frequent, unannounced basis by inserting damaged or tampered seals, or leaving a small decal or token, or tampering with the meter. Give them an immediate cash reward when the anomaly is reported.

(10) Test whether your seal installers and inspectors can be bribed.

(11) On a regular basis, security and loss prevention managers should spend a day with seal installers and inspectors, working alongside them, and listening to their comments. Managers' perceptions of the task often differ from the harsh reality.

(12) Seals that are inspected visually should be examined with an identical, unused seal held right alongside. People are not very good at remembering details of color, size, font, logos, surface texture, gloss, and patterns, but they are fairly proficient at visual side-by-side comparisons. Counterfeits can be more reliably spotted in this way.

(13) Bear in mind that tampering may involve bypassing the seal entirely. Seal installers and inspectors need to take a more holistic view than merely focusing on the seal.

(14) Most seal users are careful about protecting their seals prior to use. After use, however, seals must be archived or thoroughly destroyed--not simply thrown in the trash. Cutting a seal or punching a hole in it is NOT sufficient. Discarded seals, even if partially destroyed, provide adversaries with a useful source of information, practice samples, and counterfeit parts.

(15) Seal data, such as serial numbers, must be well protected. The data for a seal, of course, must never be stored inside a container being protected by that seal.

(16) If you can't afford outside experts to review your seals and tamper-detection program, at least seek the input of intelligent internal employees unaffiliated with the security department. It is remarkable how often smart people can detect problems in a security program that are overlooked by security personnel caught up in the day to day details of the job. Using internal employees has the additional benefit of potentially increasing security awareness throughout your organization.

(17) Security managers sometimes report that there has been no undetected tampering. That's fine if there is reliable, independent methods for detecting loss. Such a conclusion, however, is meaningless if it is based solely on seal inspections. By definition, defeated seals are never detected.

In Summary...

While seals can provide good security, the unfortunate reality is that they aren't magic. They require a lot of hard work. But what, after all, could we have expected? Effective security has always required vigilance, thoroughness, and an understanding of your organization, your weaknesses, and the threats you face. This was true even in Camelot.

Disclaimer: The views expressed in this article are those of the author and do not necessarily reflect any official position of Los Alamos National Laboratory.

About LANL

Los Alamos National Laboratory (LANL) is a multi-disciplinary research and development laboratory operated by the University of California for the United States Department of Energy. LANL was founded in 1943 as part of the Manhattan Project to create the first atomic weapons during World War II. Today, the Laboratory conducts research in a variety of technical fields. It employs nearly 10,000 people and has an annual budget of $1.2 billion.

About the VAT

The Vulnerability Assessment Team (VAT) at Los Alamos National Laboratory undertakes research and consulting in the area of tamper detection. The VAT has assisted several dozen government agencies and private companies in choosing seals, developing effective use protocols, providing training for seal installers and inspectors, setting seal standards, and conducting vulnerability assessments. The team also works at improving existing seals and developing new ones.

About the Author

Roger G. Johnston has been Team Leader of the Vulnerability Assessment Team at Los Alamos National Laboratory (LANL) since 1993. His research interests include specialty field tools, instrumentation, laser interferometry, and tamper detection. Johnston earned a B.A. from Carleton College in 1977, and M.S. and Ph.D. degrees in physics from the University of Colorado in 1983. He received his CPP certification from the American Society of Industrial Society in 1997. Prior to joining LANL, Johnston conducted research at Argonne National Laboratory, NASA, and N.V. Philips in the Netherlands.